Remote-control warfare briefing | #16

27 June 2016

Remote-control warfare is an emerging strategy that allows for conflict to be actioned at a distance. It incorporates technologies and light-footprint deployments that enable policymakers and military planners to approve actions that would unlikely be considered if using conventional means.

These monthly briefings are produced by **Open Briefing** and commissioned by the **Remote Control** project, a project of the Network for Social Change, hosted by Oxford Research Group.

Special operations forces: Coalition forces in Yemen receive reinvigorated operational and intelligence support from US special operation forces.

Private military and security companies: UN Working Group on the Use of Mercenaries recommends renewed focus on regulating PMSCs and managing foreign fighters.

Unmanned vehicles and autonomous weapons systems: Is threat to the West from drone proliferation being overblown?

Cyber conflict: Increasing awareness of risks of cyber conflict drives rise in cyber diplomacy.

Intelligence, surveillance and reconnaissance: Islamic State-linked group urges militants to secure their communications.

Special operations forces

Coalition forces in Yemen receive reinvigorated operational and intelligence support from US special operation forces

Saudi- and UAE-led coalition forces fighting both Houthi rebels and al-Qaeda in the Arabian Peninsula (AQAP) in Yemen are receiving reinvigorated operational and intelligence support from US special operations forces (SOF) to confront AQAP. Special operations forces have been redeployed to the port city of Mukalla on advisory and assistance missions to support Yemeni government forces and Arab coalition partners against AQAP militants.

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

t 020 7193 9805
info@openbriefing.org
www.openbriefing.org

Approximately 200 US SOF operators were evacuated from Yemen in February 2015 after Shia rebels captured al-Anad airbase, north of Aden, and US UAV assets were transferred to Djibouti and the United Arab Emirates. Yemen had been considered a critical counterterrorism theatre, as AQAP has demonstrated a preference for external attacks and operations, including plots against US aviation and alleged involvement in the *Charlie Hebdo* attacks. The 24th Marine Expeditionary Unit continued to provide training to Saudi and UAE forces until April 2015.

US Central Command (CENTCOM) recently indicated that its key objective is to deny AQAP safe haven in Yemen and degrade and disrupt the organisation.[1] The increasing tempo of air strikes against AQAP, which CENTCOM puts at nine strikes,[2] though the Long War Journal has recorded 18 for 2016 so far,[3] is consistent with the reestablishment of SOF advisory and assistance missions. However, air strikes alone have not paved the way for the redeployment of US special operations forces. An extremely fragile and tentative ceasefire between the government of Abd Rabbuh Mansur Hadi and Houthi rebels has also opened up a space for UAE, Saudi and US special forces to resume counterterrorism operations against AQAP.

US assistance to coalition forces is likely to involve aerial surveillance, mission planning, medical assistance, marine interdiction and logistical support. A navy amphibious assault ship with more than 1,200 marines is stationed offshore in the Gulf of Aden to provide medical support. While coalition and Yemeni government forces have wrestled control of Mukulla from AQAP, the port city is far from secure: a Yemeni affiliate of Islamic State launched a suicide bomb attack at a Yemeni naval base in the city on 12 May. Similarly, the fragile ceasefire could unravel, forcing UAE and Saudi Arabian forces to again focus on the rebels and creating an opportunity for AQAP to regroup.

The counterterrorism strategy against AQAP may buy the US administration and its Gulf allies time, but is unlikely to significantly degrade and disrupt the group. Yemen's broader sectarian conflict needs political resolution as a foundation for an effective counterterrorism operation against AQAP. In the meantime, US special operations forces risk being perceived as fighting the Houthi rebels if the lines become blurred, as Yemeni government forces are fighting on two fronts against both Houthi rebels and AQAP militants.

[1] http://www.longwarjournal.org/archives/2016/06/us-military-announces-3-new-airstrikes-in-yemen.php

[2] http://www.defense.gov/News-Article-View/Article/790791/centcom-announces-yemen-counterterrorism-strikes

[3] http://www.centcom.mil/news/press-release/june-3-u.s.-central-command-announces-yemen-counterterrorism-strikes?utm_source=Sailthru&utm_medium=email&utm_campaign=New%20Campaign&utm_term=%2ASituation%20Report

Other developments

Key NATO powers and Middle Eastern allies are negotiating deployment to and intervention in Libya to prevent IS forces taking a foothold in the politically-fractured country. The chairman of the US Joint Chiefs of Staff, General Joseph Dunford, was in Brussels negotiating expanding SOF advise and assist missions with European partners in mid May according to anonymous Pentagon officials.[4] While much has been is made of these negotiations, Italian, Jordanian, British and US special operations forces are already operating in Libya. Reports of strikes by UK special forces and the electronic jamming of IS communication networks by RAF Rivet Joint spy planes have thrown doubts on official comments about British involvement in Libya. The head of the UK parliamentary foreign affairs committee, Crispin Blunt, had sought clarification on the UK deployment,[5] and the Secretary of State for Defence, Michael Fallon, indicated on 24 May that there were no plans for a UK combat role in Libya.[6]

US special operation forces working with Kurdish People's Protection Units (YPG) forces in Iraq and Syria have been asked to remove YPG patches from their uniforms. The US Department of Defense initially argued that the patches were to help US forces blend in; however, this position was reversed after the Turkish foreign minister, Mevlüt Çavuşoğlu, suggested it was hypocritical, as Turkey lists the YPG as a terrorist organisation. The Pentagon's initial defence of soldiers needing to 'blend in' may suggest a degree of mission creep, with US SOF more likely to be on the frontlines or playing a combat role despite repeated US assurances to contrary. Ankara's concern over the insignia and cooperation between US and Kurdish forces is likely the motivation for Ankara's offer of joint Turkish-US SOF counter-terrorism operations in Syria, which was made on the condition that Kurdish forces cannot be part of the deal.

The annual Special Operations Forces Industry Conference (SOFIC) was held in Tampa, Florida, on 23 to 26 May. In a keynote speech, the new commander of US Special Operations Command (USSOCOM), General Raymond A. Thomas III, outlined his vision of special operations as highly technologically-enabled proactive forces. At the centre of Thomas's speech was the idea the special operations forces, particularly US SOF, are in a highly kinetic phase in response to instability in multiple failed states, and that with future stabilisation, special operations would focus more on pre-emptive, quasi-intelligence activities.[7] An anticipatory posture that worked to diffuse crises before they materialised would include a 'transregional assessment process' that sought to understand the underpinning social, environmental and economic drivers of conflict devoid of specific geographic features.

[4] http://www.washingtonexaminer.com/u.s.-readies-expansion-of-counter-isis-effort-in-libya/article/2591893

[5] https://www.parliament.uk/documents/commons-committees/foreign-affairs/Correspondence/2015-20-Parliament/Letter-to-Foreign-Secretary-160315-Libya.pdf

[6] http://www.middleeasteye.net/news/uk-not-planning-any-kind-combat-role-libya-defense-secretary-211719996

[7] http://www.defenseone.com/threats/2016/05/americas-new-special-operations-commander-wants-predict-future/128583/

Also of note

- **The Somali Army and US SOF advisors conducted a raid on 31 May that may have killed the suspected al-Shabaab planner of the Garissa University College attack in Kenya.** Two weeks earlier, US operators called in an airstrike on al-Shabaab militants west of the Somali capital, Mogadishu, after Ugandan troops came under fire.
- **Tunisian special forces killed a senior commander of local IS-affiliate Jund al-Khilafah in the country's central, mountainous region on 18 May.** This comes at the same time as news that Tunisian IS commanders in Libya have set up training camps in preparation for attacks in Tunisia. Meanwhile, elite Tunisian police squads disrupted a major planned attack in the capital, Tunis.
- **Russian political and military strategists are weighing up deploying more special forces for ground combat operations in Syria to help fight rebel groups,** believing a final decisive ground battle is required to end the conflict.[8] In late April, Russia's deputy foreign minister, Sergei Ryabkov, suggested that US special operations forces were violating Syrian sovereignty.
- **A joint Afghan-US SOF kill or capture mission turned into a hostage rescue in mid-May.** The team rescued Ali Haider Gilani, the son of former Pakistani prime minister Yousuf Raza Gillani, during a raid on an al-Qaeda compound near the Pakistani border. Earlier in the month, Afghan-US special forces freed over 60 Taliban prisoners in Helmand province.
- **North Korean special forces were reportedly taking part in joint exercises with Venezuelan special forces (Groupo de Acciones Commando) in Caracas, Venezuela, in May.** There are also reports that Cuban military personnel and the 21st Armed Group of the People's Liberation Army (PLA) are temporarily stationed with the Venezuelan Ministry of Defence for the joint exercises.
- **Approximately 1,500 of Iraq's Counter-Terrorism Service special forces personnel are amassing around Fallujah in preparation to retake the IS-held city west of Baghdad.** The Iraqi prime minister, Haider al-Abadi, told parliament on 29 May that the offensive to recapture the city will begin at the end of the current second phase.
- **The commander of US Special Operations Command, Pacific (SOCPAC), Rear Admiral Colin Kilrain, told Reuters that he had discussed military-to-military cooperation and training with the commander of Vietnam's elite forces** on the sidelines of the 2016 Special Operation Forces Industry Conference (SOFIC) in Tampa, Florida. The discussion came as the US president, Barack Obama, ended the US embargo on arms sales to Vietnam.

[8] http://www.aljazeera.com/news/2016/06/russian-ground-operation-syria-160602094724997.html

Private military and security companies

UN Working Group on the Use of Mercenaries recommends renewed focus on regulating PMSCs and managing foreign fighters

Operating under the UN Office of the High Commissioner, the EU institutions mission of the UN Working Group on the Use of Mercenaries has advocated that key EU institutions consider increased and more-effective regulation of private military and security companies (PMSCs) and evaluate compliance with international law for measures aimed at foreign fighters.[9]

The European Union and 23 of its 28 member states have signed the Montreux Document, which requires the application of international law to the use and activities of PMSCs and creates a code of conduct for PMSCs. Those companies failing to meet this code of conduct are blacklisted, and the EU (and other signatories) refuse to employ their services. The Working Group identified other EU legal mechanisms and measures that are or could be used to better regulate PMSCs and influence the PMSC market. These include the European Court of Justice ruling that PMSCs form an economic sector, giving the European Commission competency under first pillar rules, which govern economic and social activity within the European Union. However, the EU Council, in response to lobbying from PMSCs, did not include the sector in the internal market – essentially deregulating the sector.

EU member states currently employ PMSCs to support civilian, police and military missions. The police and civil deployment of PMSCs is generally limited to close protection functions in Palestine, the former Yugoslavia and Congo missions. PMSCs support military missions in various African countries, the Mediterranean, anti-piracy missions in the Gulf of Aden and the former Yugoslavia countries. They are not recruited by the EU, but rather by individual countries in accordance with national law.

The European Parliament has expressed concern over the use of PMSCs, and has expressed a desire for the EU to create a harmonised list of security and military services and a code of conduct – including a minimum set of standards – designed to address several problems before they occur. Such problems include decreased democratic control, lack of accountability and contractor impunity.

The differences in opinion of the legal, parliamentary and head of states institutions within the European Union over the use of PMSCs and their regulation has inspired the UN working group to considered whether the EU should, and could, regulate the PMSC sector. The working group is now looking at both the political and procurement challenges surrounding the sector. This will allow the EU to look at ways of potentially regulating the market under the services directive. This could come in the form of national, EU, other international or voluntary regulations. The EU Parliament's Sub-Committee on Security and Defence (SEDE) is considering an own-initiative report (INI) regarding the sector.

[9] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=19914&LangID=E

Other developments

The extent of PMSC and other contractor support to US counterterrorism deployments suggests that light-footprint operations may not be as small-scale as the US administration describes them.[10] PMSCs remain a critical component of the United States' light-footprint global counterterrorism deployments. Contractor support figures for Q2 2016 released by US CENTCOM show that CENTCOM currently has over 44,000 contractors deployed, with Afghanistan having the lion's share of the deployment.[11] In all CENTCOM theatres of operation, the overwhelming majority of contractors continue to be from outside the country they are deployed to, with nearly 72% being US citizens or from third-party countries. Local and domestic contractors make up only 28% of contractors. Contractors also appear to have a higher casualty rate than US troops: between 2009 and 2016, 1,540 contractors were killed in Iraq and Afghanistan compared to 1,301 US troops.

Iranian recruiters are allegedly seeking out foreign Shiite fighters for battles in Syria. Reports suggest that Iran has opened a recruitment centre in Herat, Afghanistan, to secure foreign fighters for the conflict in Syria.[12] On 7 June 2016, Iran released a propaganda video aimed at increasing the recruitment of foreign mercenaries into Syria.[13] The video specifically targets Afghan mercenaries to join the Fatemiyoun Brigade – a predominately Shia Afghan militia fighting in Syria. Fatemiyoun is thought to have around 20,000 fighters. Commanders from both Iranian brigades and the Fatemiyoun brigade have been photographed together[14] and have attended the funerals of their counterparts. The economic inducements and incentives for Afghan fighters are significant and include a chance of Iranian citizenship, money and property if they agree to fight in Syria for mercenary groups supporting the Assad regime.[15]

In early May, the Democratic Republic of Congo (DRC) announced a crackdown on the operations of foreign mercenaries in the country. The crackdown comes after the government made allegations that Moise Katumbi, the main opposition leader, was hiring foreign mercenaries to overthrow the current president, Joseph Kabila. On 19 May 2016, Katumbi announced he would be running for the presidency; on the same day, the DRC government issued an arrest warrant for him for allegedly hiring mercenaries as part of an alleged plot to topple the president.[16] Presidential elections are scheduled for November 2016, but there are growing fears that Kabila may not step down at the end of his mandated two terms. Under DRC law, a PMSC must seek approval from several government departments before they are allowed to operate in the country, must not be used as a replacement for the police or military, and are banned from carrying firearms. As part of its investigation, the government has been investigating Pomba 1, based in Katanga province. The company has been linked by the government to the recruitment of foreign mercenaries and has allegedly failed to register with the correct government departments.[17]

[10] http://foreignpolicy.com/2016/05/18/private-contractors-are-the-silent-majority-of-obamas-military-mercenaries-iraq-afghanistan/

[11] http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_April2016_Final.pdf

[12] http://www.csmonitor.com/World/Middle-East/2016/0612/Iran-steps-up-recruitment-of-Shiite-mercenaries-for-Syrian-war and https://news.vice.com/article/afghan-refugees-and-jihadis-are-reportedly-fighting-on-opposite-sides-of-syrias-war

[13] https://www.youtube.com/watch?v=nAqRHG8-e3I

[14] http://www.longwarjournal.org/archives/2015/03/analysis-shiite-afghan-casualties-of-the-war-in-syria.php

[15] http://www.csmonitor.com/World/Middle-East/2016/0612/Iran-steps-up-recruitment-of-Shiite-mercenaries-for-Syrian-war

[16] https://next.ft.com/content/4cbb6082-1dd8-11e6-b286-cddde55ca122 and http://uk.reuters.com/article/congodemocratic-politics-idUKL5N18283F

[17] http://www.aljazeera.com/news/2016/05/dr-congo-cracks-foreign-mercenaries-160504150108710.html

Also of note

- **Details have been released of a deal signed between Reflex Response (R2) – an Abu Dubai based PMSC – and the United Arab Emirates.** The $529 million deal contracts R2 to supply PMSC services to Yemen to underpin Gulf Cooperation Council in-country operations in support of President Abd Rabbuh Mansur Hadi. R2, whose creation was associated with Erik Prince, founder of Blackwater (now Academi), is reported to have hired 15 Academi personnel to support the operation.[18]
- **Uganda's top export is now considered to private military and security services.** The country now exports 1,000 PMSC contractors every month according to Interpol. There are approximately 20,000 Ugandan mercenaries currently serving abroad. [19]

[18] http://www.presstv.ir/Detail/2016/05/26/467545/UAE-Yemen-Saudi-Arabia-Taizz and https://www.almasdarnews.com/article/mercenary-group-yemen-identified/?utm_source=rss&utm_medium=rss

[19] https://www.issafrica.org/chapter-one-private-and-public-security-in-uganda-solomon-wilson-kirunda and http://answersafrica.com/ugandas-greatest-export-mercenaries.html and http://www.bloomberg.com/features/2016-uganda-mercenaries/

Unmanned vehicles and autonomous weapons systems

Is threat to the West from drone proliferation being overblown?

In an article for The Diplomat, two Italian security researchers, Andrea and Mauro Gilli, have argued that the rapid increase in the proliferation of drones around the world is not the threat to global security and Western primacy that many analysts are forecasting.[20]

Despite over 80 countries now possessing drone technology,[21] the researchers rightly point out that the overwhelming majority of the drones used worldwide are low-performance, low-ability surveillance platforms, with minimal offensive capabilities. The authors claim that concerns that hostile forces are catching up with Western militaries in terms of drone capability are unfounded. The developments the United States in particular is making in terms of stealth, speed, offensive capabilities and fully-autonomous operation are simply not being matched in other parts of the world. Of potentially-hostile countries, Russia is struggling to develop a combat-capable drone that can target a moving armoured target with confidence. And China is making progress in surveillance technology, but is also struggling to make headway with compatible missile technology. Other than these two major powers, there are no countries that are anywhere close in terms of drone developments.

However, such arguments ignore the fact that while these drones are basic *now*, their capabilities will almost certainly rapidly develop (especially with the exponential growth in micro-technology), much as Western platforms have since their origins. Also, while Western drones can operate strategically over thousands of miles, this capability is not necessary in modern warfare, especially the unconventional warfare seen around the world today.

Tactical drone operations, involving basic platforms launched by units on or near the frontline, can already fulfil the operational surveillance and strike requirements of field commanders. For example, Azerbaijan has already conducted suicide drone strikes on Armenian forces using platforms that can be self- or manually-guided onto their targets.[22] These are almost certainly cheaper than most Western models, and do not need the complex support infrastructure required for the likes of MQ-9 Reapers. And while the United States is investing vast sums in developing swarm capabilities involving multiple complex drones with only one human operator, less-developed militaries can deploy weaponised drones using multiple pilots instead.

The authors argue, however, that the more basic a drone, the easier it is to defend against it, pointing out that they can be vulnerable to small arms fire and off-the-shelf software. While there is truth in this, it ignores the fact that such aircraft are small, agile and can operate at altitudes that would make them very difficult to shoot down with personal infantry weapons. Software countermeasures may work in the short term, but drone command signals can almost certainly be protected by counter-countermeasure software. In any case, software countermeasures would need to widely issued across the military to provide effective cover.

[20] http://thediplomat.com/2016/05/why-concerns-over-drone-proliferation-are-overblown/

[21] http://foreignpolicy.com/2013/03/11/the-global-swarm/

[22] https://warisboring.com/azerbaijan-kills-armenian-troops-with-a-suicide-drone-b8cf2263ed93#.v6c57m43j

Other developments

Islamic State's (IS) use of drone technology has developed at a steady pace over the last year or so. In late 2014, the group used unmanned aerial vehicles (UAVs) to shoot aerial imagery of Kobane, Syria.[23] In March 2015, coalition forces reported sightings of UAVs being used to conduct reconnaissance operations near Fallujah, Iraq.[24] In December 2015, Kurdish Peshmerga forces claimed to have seen evidence of weaponised UAVs.[25] In April this year, there were reports of Islamic State using drones to carry out chemical attacks on Kurdish groups.[26] Now plans have been found on the laptop of Salah Abdeslam, the mastermind of the November 2015 Paris terrorist attacks, to use drones to carry out an attack on the recent England vs. Russia football match at the UEFA Euro 2016 in France. Both countries are heavily involved in attacks on IS operations in Syria, and this would have been a major propaganda coup if the attack had taken place. Security chiefs are becoming increasingly concerned that this summer provides multiple crowded events and tourist locations that could be targeted using drones.

New open-source satellite imagery recently confirmed that China has deployed one of its latest stealth-technology drone to one of its bases in the South China Sea.[27] The imagery, from ImageSat International, shows a Harbin BZK-005 long-range reconnaissance drone, capable of loiter times of up to 40 hours, on Woody Island in the north of the region. This high-altitude long-endurance (HALE) model is China's equivalent of the United States' Global Hawk.[28] Should it remain in the region, the UAV will possibly be used to monitor the US Navy's 7th Fleet, which is highly active in the area conducting freedom of navigation patrols through the waters, to China's increasing anger. China has yet to deploy combat aircraft to the newly-built artificial islands in the Spratly Island group further south. While this would be considered antagonistic and confrontational in the current climate, deploying fighters and combat drones in the near-future is not inconceivable.

The US Navy has moved ahead with plans to deploy autonomous surveillance and combat UAVs from submarines.[29] The Blackwing drone, built by Californian-based AeroVironment, is small and laden with advanced capabilities more usually seen in larger aircraft, including electro-optical and infrared sensors. It can be launched from a submerged submarine's torpedo tubes. The navy has requested funding to purchase 150 Blackwings, which are seen as a solution to the emerging threat of anti-access/area-denial (A2/AD) weapons, such as long-range anti-ship missiles, being developed by the likes of China. Submarines fitted with surveillance-capable Blackwings will now be capable of conducting such surveillance operations in greater safety. Blackwing drones can also be deployed from surface vessels and ground vehicles, greatly increasing their military use. In other developments, a seven-metre torpedo-like drone designed to loiter at depths of 6,000 metres for years at a time while awaiting activation and tasking has been developed by the United States' Defense Advanced Research Projects Agency (DARPA).[30]

[23] http://www.dailymail.co.uk/news/article-2871389/ISIS-propaganda-Call-Duty-style-Latest-footage-shows-drone-s-view-battle-ravaged-streets-Kobane-swooping-gun-battles-ground.html

[24] http://foreignpolicy.com/2016/04/28/terrorists-have-drones-now-thanks-obama-warfare-isis-syria-terrorism/

[25] http://foreignpolicy.com/2016/04/28/terrorists-have-drones-now-thanks-obama-warfare-isis-syria-terrorism/

[26] http://foreignpolicy.com/2016/04/22/isis-is-using-chemical-weapons-against-the-kurds-why-wont-the-u-s-help/

[27] https://seasresearch.wordpress.com/2016/05/27/update-2-new-satellite-imagery-shows-chinese-drone-on-woody-island/

[28] http://thediplomat.com/2016/06/south-china-sea-chinas-surveillance-drones-make-it-to-woody-island/

[29] www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2182

[30] http://www.janes.com/article/60320/darpa-s-shark-completes-at-sea-testing

Also of note

- **Nigeria is reportedly working hard to have guided missile systems fitted to its UAV fleet.**[31] The country's military leadership is working on a partnership with the Nigerian Space Research and Development Agency (NASRDA) to develop missile and rocket technology.
- **IS forces in Raqqa, Syria, have started covering streets with sheets slung between buildings in a bid to protect its personnel against drone strikes.**[32] This low-tech tactic has also been seen in Ramadi and other IS-held cities. While thermal cameras and sensors on drones can detect people through the sheets, they cannot positively identify individuals for targeting.
- **A British system capable of jamming signals to small drones is to be trialled by the US Federal Aviation Authority.**[33] AUDS (Anti-UAV Defence System) works by jamming signals to drones, making them unresponsive, and will be tested at several airports selected by the FAA.
- **The Taliban leader, Mullah Akhtar Mohammed Mansour, is reported to have been killed in a drone strike on 21 May.**[34] The strike took place southwest of the town of Ahmad Wal on the Pakistani-Afghan border.

[31] http://allafrica.com/stories/201605250104.html

[32] http://www.newsweek.com/isis-covering-streets-raqqa-thwart-drone-strikes-452943 and https://twitter.com/Raqqa_SL/status/725111867786559488/photo/1.

[33] http://www.bbc.co.uk/news/technology-36425879

[34] http://www.theatlantic.com/international/archive/2016/05/targeting-the-talibans-leader/483833/

Cyber conflict

Increasing awareness of risks of cyber conflict drives rise in cyber diplomacy

In the last month, a number of major powers have participated in dialogues and diplomacy around cyber issues and telegraphed important political messages to allies and adversaries alike.

The recent G7 leaders summit on 26 May endorsed the G7 Principles and Actions on Cyber,[35] and outlined key objectives around internet governance and cyber security.[36] The principles and G7 communiqué emphasise openness, security, interoperability, the free flow of information and the protection of human rights and the rule of law online, and reiterate that under some circumstances cyber activities may amount to a use of force. The G7 cyber narrative appears to intentionally emphasise values potentially at odds with the cyber sovereignty rhetoric and doctrines used by Russia and China.[37]

This supposed polarisation was reinforced days later by the US defence secretary, Ash Carter, who told the Shangri-La Dialogue 2016 meeting on 4 June that the Asia-Pacific region is experiencing greater anxieties around China's activities in cyberspace.[38] The comments largely echoed the April 2016 report from the Pentagon on China's cyberwarfare capability and activities, which noted alleged Chinese cyber activities against the US Department of Defense and potential Sino aspirations to map and understand defence networks, logistics and capabilities.[39] Similarly, the testimony of the US state department before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy highlighted the United States' interpretation of China's cyber policy as predominately focused on 'maintaining internal stability, maintaining sovereignty over its domestic cyberspace, and combating what it argues is an emerging cyber arms race and "militarization" of cyberspace.'[40]

This resurgent focus on cyber diplomacy is driven by a broad range of political, technological and social forces; however, the disruption of Ukraine's electricity distribution network and the US Cyber Command's campaign against Islamic State have brought offensive cyber capabilities to the forefront of international discussions. The chief research officer for the cyber security company F-Secure, Mikko Hyppönen, has suggested the global environment is 'switching from cyber espionage to offensive cyber action'.[41]

[35] http://www.mofa.go.jp/files/000160279.pdf

[36] http://www.mofa.go.jp/files/000160266.pdf

[37] http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/ and http://www.huffingtonpost.com/scott-malcomson/russia-china-internet_b_9841670.html

[38] https://www.iiss.org/en/events/shangri%20la%20dialogue/archive/shangri-la-dialogue-2016-4a4b/plenary1-ab09/carter-1610

[39] http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf

[40] http://www.foreign.senate.gov/imo/media/doc/052516_Painter_Testimony.pdf

[41] http://www.theregister.co.uk/2016/06/06/f_secure_cyberwar_iii/

With greater exposure to and public awareness of the cyber threat, politicians are also pushing cyber norms and preparation at the domestic level. In the United States, Senator Mike Rounds, a member of the Senate Armed Services Committee, introduced the Cyber Act of War Act (2016) on 9 May.[42] The bill requires the US administration to define what would constitute an act of war in cyberspace and the appropriateness of countermeasures.[43] The Republican senator argues that the United State can more effectively develop cyber deterrence and proactive policies with a clear signal of what constitutes a cyber-enabled act of war.

Across the Atlantic, the Conservative MP Sir Nicholas Soames asked the British defence secretary about whether there is a definition of a cyber act of war.[44] The UK government's response was that cyber activity constitutes an armed attack if the consequences are 'essentially the same as those of a conventional kinetic attack'. The UK government also makes a distinction between a cyber criminal act and a cyber armed attack based on scale of impact.

The head of Germany's cyber command, Major General Ludwig Leinhos, told a conference at the Berlin air show that he expected NATO members to agree to designate cyber as an official operational domain of warfare at the July Warsaw summit.[45] While the asymmetrical cyber capabilities of Russia are likely to have spooked NATO partners into developing doctrine, governance and capability, there are other possible drivers of the designation: China, North Korea and Iran have significant offensive cyber capabilities.[46] The designation is likely to open the door for greater dialogue, intelligence sharing and joint training exercises. However, challenges around attribution and proportionality of response, as noted in previous Article 5 discussions, remain unresolved.

Discussions of this nature are likely to increase in frequency as global powers seek to build alliances for operational cooperation and norm building around cyber issues. The NATO designation of cyber as a domain of warfare will accelerate existing cooperation activities, which will in turn spur key adversarial cyber powers, such as Russia and China, to pursue alternative cyber alliances.

Other developments

There is speculation that Iran and Saudi Arabia are engaged in low-lever cyber intrusions and attacks on each other's IT infrastructure after hackers compromised government websites it both countries. The tit-for-tat cyber exchange started on 24-25 May when the Statistical Centre of Iran website was compromised. Two days later, the Saudi Arabian Statistics Centre government website was attacked. Iranian foreign ministry websites experienced subsequent attacks, which Iran's Cyber Police (FATA) indicated originated from IP addresses in Saudi Arabia. The low-level cyber intrusions possibly reflect the poor state of relations between Iran and Saudi Arabia. The head of Iran's Civil Defence Organisation has reportedly previously warned that Saudi Arabia was planning cyber attacks against Iran and that Iran was undertaking cyber war games to improve its defensive capabilities.

[42] https://www.congress.gov/bill/114th-congress/senate-bill/2905/text

[43] http://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124

[44] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-05-18/37120

[45] http://www.reuters.com/article/us-cyber-nato-germany-idUSKCN0YN46R

[46] https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

The US administration continues to keep details of cyber operations against Islamic State out of the public domain, with Colonel Steve Warren, spokesperson for Operation Inherent Resolve, telling a Q&A forum on the Reddit social network the 'first rule of cyber operations: never talk about cyber operations'.[47] However, the US defence secretary, Ashton Carter, told reporters in California that other countries possess the type of offensive cyber weapons the United States is employing against Islamic State.[48] Carter used this point to emphasis the idea that the administration's focus on cyber security is necessary considering the fact that potential US adversaries also possess a disruptive cyber arsenal. The reticence to reveal the cyber tactics and tools the United States is using against Islamic State arises from fears that the group may develop countermeasures and that other adversaries may use the US operations as precedent for discussions about what constitutes a cyber act of war or adversely impact US diplomacy around cyber norms. Further revelations may unveil a significant mismatch between the sophistication of US cyber offensives and the actual cyber capabilities and ICT network security of Islamic State.[49]

The German Federal Office for the Protection of the Constitution (BfV) has identified an allegedly Russian threat actor group, Sofacy, as responsible for an advanced persistent threat (APT) campaign that shut down the computer network of the Bundestag's lower house in June 2015. The president of BfV, Hans-Georg Maaßen, stated that Russian intelligence agencies had recently shown a willingness to go beyond accessing classified data and were conducting sabotage campaigns.[50] The campaign comes as Russian and German relations have hit a low point following Russia's annexation of Crimea and intervention in Syria.

Also of note

- **Cybersecurity company FireEye reported that the website of Taiwan's Democratic Progressive Party (DPP) was redirected to a fake website in order to collect information on website visitors.** The company suggested that hackers from China were most likely behind the attack, as Beijing is concerned that the newly-elected DPP may move away from the pro-mainland policies pursued by the previous government.
- **The UK minister for the Cabinet Office, Matt Hancock, delivered a speech on 25 May outlining the UK government's cyber security strategy, including the establishment of the National Cyber Security Centre (NCSC).** The NCSC will service both industry and government and build upon the expertise of the Centre for the Protection of National Infrastructure, Cert-UK, the Centre for Cyber Assessment and the information security arm of GCHQ.
- **South Korea has claimed that North Korea's Bureau 121 of the General Bureau of Reconnaissance launched a cyber attack against a navy defence contractor that produces Seoul's naval vessels and amphibious assault vehicles.** The attack is likely linked to North Korea's concerns about the attack capabilities of South Korea's rapid amphibious special operations forces.

[47] https://m.reddit.com/r/IAmA/comments/4i5r4h/hey_reddit_im_col_steve_warren_spokesman_for/

[48] http://www.reuters.com/article/us-cyber-defense-isis-idUSKCN0Y302F

[49] https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.diKaZdL1V#.elePDo5LN and https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf

[50] http://www.wsj.com/articles/germany-points-finger-at-russia-over-parliament-hacking-attack-1463151250

- **Symantec has suggested that the code used in cyber robberies of Bangladeshi, Vietnamese and Filipino banks was similar to code used by the Lazarus threat actor,** which is accused of various attacks on the United States and South Korea. If the attacks are attributable to state-sponsored threat actors in North Korea, it would suggest that the economic pressures on Kim Jong-un's regime are significant.
- **The European Council has issued a new network and information security (NIS) directive requiring essential services, critical infrastructure and digital service providers to reduce cyber attack risks and report major incidents.** To support the directive, EU member states agreed to create a new network of national computer security incident response teams.

Intelligence, surveillance and reconnaissance

Islamic State-linked group urges militants to secure their communications

Islamic State (IS) has published a new series of manuals to help IS supporters and fighters use new technology to keep their communications hidden from intelligence agencies. It is thought that the group is becoming increasingly concerned about the effectiveness of communications intercept operations by Western agencies.

One group linked to Islamic State, the Horizon Electronic Foundation (HEF), has drafted five Arabic-language manuals and distributed them along secure channels using the Telegram messaging service.[51] This group was first noted in February 2016, and has been very active in urging militants to make efforts to secure their communications both within Syria and Iraq and beyond. It suggests using Virtual Private Networks, the TOR Browser (which covers the IP address tracks of internet users) and encrypted email servers, such as ProtonMail. HEF advises avoiding US-based applications that can be accessed by US agencies, naming Google and Yahoo as examples. HEF also provides recommendations for several security and privacy apps available for smartphones.[52] Security agencies will no doubt start targeting the named apps to identify and access IS-related communications where possible.

This is not an entirely new development. Militants have been noted using encrypting software in the recent past, with French-based groups found to be using TrueCrypt for their communications in March 2016. The deputy director of the NSA, Richard Ledgett, recently assessed the IS leadership to be incredibly 'OPSEC savvy.'[53] One principal reason for this is that Islamic State's leadership includes a large number of veterans from the fighting in Iraq, where they gained a detailed insight into the intelligence gathering techniques and capabilities of Western agencies.[54]

Frustratingly, the US-led coalition is already suffering from a growing shortage of effective intelligence assets according to Lt. Gen. Charles Q. Brown, the US commander of the air war in Syria and Iraq.[55] He is increasingly relying on surveillance drones and other airborne assets (many provided by UK forces) to find ad hoc opportunist targets ('dynamic targeting') as communication intelligence sources struggle to pinpoint targets.[56] This needs to be reversed and a return made to intelligence-led deliberate targeting.

[51] http://www.csmonitor.com/World/Passcode/2016/0520/How-Islamic-State-militants-attempt-to-outwit-spies?mc_cid=950476ba62&mc_eid=0a14282483

[52] http://www.csmonitor.com/World/Passcode/2016/0520/How-Islamic-State-militants-attempt-to-outwit-spies?mc_cid=950476ba62&mc_eid=0a14282483

[53] https://stream.org/top-nsa-official-isis-leadership-incredibly-security-savvy/

[54] https://stream.org/top-nsa-official-isis-leadership-incredibly-security-savvy/

[55] http://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets

[56] http://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets

A new line of attack against Islamic State was recently initiated when the US administration directed US Cyber Command (USCYBERCOM) to carry out network attacks on the group's communication systems.[57] The West enjoys a somewhat substantial advantage in cyberwarfare technology and capability, and Islamic State's increasing efforts in this field have now motivated the West to respond with a major cyber offensive. This will target the core body's command, communications and intelligence structure in the Middle East, but also the links to support groups and sympathisers in Europe and North America.[58] IS-linked groups in Libya are also expected to be targeted.[59] Operations will include remote hacking of computers and smartphones and implanting tracking and disruptive viruses, which will provide intelligence on messages and movements as well as obstruct communications.[60]

Western cyber operations will also need to involve defensive, as well as offensive, strategies. There is growing evidence that IS sympathisers are targeting Western computer systems, carrying out their own disruptive attacks on the sites and networks of governments, security and intelligence agencies and businesses.

Other developments

Twitter has blocked the US government from using a Dataminr product to mine its data. Dataminr's core product scours social media, identifying patterns that point towards significant events using complex algorithms that pick up on context and common keywords and create alerts. Until now, this had been used extensively by several US security, law enforcement and defence agencies.[61] The value of this application was demonstrated when it alerted US intelligence agencies to last year's terrorist attacks in Paris within five minutes of them taking place, 45 minutes before the news broke on Associated Press.[62] Government agencies had been indirect investors in the app alongside Twitter, which has a 5% stake. This included a pilot access scheme that Twitter concluded.[63] Twitter's leverage comes from Dataminr needing access to Twitter's feeds for source data – without Twitter the app is all but useless. Twitter's goals are still unclear, but this may be a stand in defence of user privacy and against mass surveillance. The US government is not entirely shut out, as the Department of Homeland Security has a contract with Dataminr that is not affected by this lockout.

[57] http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html and http://uk.businessinsider.com/new-us-cyber-war-against-isis-2016-4?r=US&IR=T

[58] http://uk.businessinsider.com/new-us-cyber-war-against-isis-2016-4?r=US&IR=T

[59] http://www.rand.org/blog/2016/02/the-three-challenges-of-countering-isis-in-libya.html

[60] http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0518/Opinion-The-case-for-launching-a-digital-invasion-against-ISIS?mc_cid=592ae1f47c&m%E2%80%A6

[61] https://www.wired.com/2016/05/twitter-dataminr-intelligence-community/ and http://www.delawareonline.com/story/opinion/contributors/2016/05/13/twitters-stand-surveillance-endangers-united-states/84340632/

[62] http://fortune.com/2016/04/15/cia-investment-portfolio/

[63] http://www.delawareonline.com/story/opinion/contributors/2016/05/13/twitters-stand-surveillance-endangers-united-states/84340632/ and https://www.wired.com/2016/05/twitter-dataminr-intelligence-community/

The FBI look set to gain new powers in a new clause added to an upcoming Senate Bill. The Bill, the Senate Intelligence Authorization Act, which primarily re-authorises intelligence agencies' surveillance powers, includes an additional provision that will give the FBI the power to demand warrantless access to citizens' email and browsing histories via a tool called National Security Letters.[64] This tool was routinely used to access email and browsing histories without a warrant until 2008, when the Department of Justice declared that these were no longer permitted and such data required a court order (though the FBI is reported to have continued regardless, using a different legal interpretation[65]).[66] The major technology and communications corporations have been fighting the FBI's requests since then by refusing to provide email metadata and online records. The FBI have seemingly grown weary of the constant fight, and have chosen to find a conclusive legislative solution.[67]

In a new file from Edward Snowden, it appears that UK intelligence agencies were becoming concerned about a 'data glut' in 2010. The report, marked UK Secret and dated 21 February 2010, was apparently prepared by Security Service (MI5) officials for a briefing to the UK Cabinet Office and HM Treasury on DIGINT surveillance capabilities.[68] So much data was being collected by the agencies that chiefs were worried that vital intelligence would be overlooked.[69] This fear was realised three years after the report when two extremists killed and attempted to decapitate a British soldier on a London street. Both perpetrators were known to the Security Service, but vital warning intelligence indicators were missed, including phone calls to an al-Qaeda-affiliated group in Yemen and social media posts in which one of the individuals described in graphic detail his intention to murder a soldier in the United Kingdom. [70] The report has been released by the Intercept website to coincide with the Investigatory Powers Bill progressing through the parliamentary legislative process. The Bill, which is now at the report stage in parliament, aims to give legal authority to the bulk collection of internet traffic, as well as requiring communications providers to store browsing records for 12 months.[71]

[64] https://boingboing.net/2016/05/27/someone-just-snuck-warrantless.html and https://theintercept.com/2016/06/07/new-intelligence-bill-gives-fbi-more-secret-surveillance-power/

[65] https://theintercept.com/2016/06/02/fbi-kept-demanding-email-records-despite-doj-saying-it-needed-a-warrant/

[66] https://theintercept.com/2016/06/07/new-intelligence-bill-gives-fbi-more-secret-surveillance-power/

[67] https://theintercept.com/2016/06/07/new-intelligence-bill-gives-fbi-more-secret-surveillance-power/

[68] https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/ and https://theintercept.com/document/2016/06/07/digint-narrative/

[69] https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/, http://www.bbc.com/news/technology-36469351 and https://theintercept.com/document/2016/06/07/digint-narrative/

[70] https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/

[71] http://www.bbc.co.uk/news/technology-36469351

Also of note

- **GCHQ and the NSA have access to intercepted emails sent and received by all British MPs, including those with their constituents, according to a *Computer Weekly* investigation.**[72] Parliamentary emails are transmitted via overseas datacentres allowing them to be intercepted by Tempora, GCHQ's bulk collection operation.
- **Repressive governments around the world are turning to US commercial software to monitor and intimidate dissidents.**[73] Due to weak regulation, any government can purchase US spyware that can monitor a target's messages, calls and location.
- **An open-source initiative aims to map where state-sponsored malware has been used to target citizens.**[74] Digital Freedom Alliance, a collaboration of security researchers, has launched the app to quantify government attacks against journalists, activists, lawyers and NGOs around the world.

Commissioned by the Remote Control Project

remotecontrolproject.org

REMOTE CONTROL
Examining changes in military engagement

[72] http://www.computerweekly.com/news/450297574/MPs-private-emails-are-routinely-accessed-by-GCHQ?mc_cid=9ee4c3dc11&mc_eid=0a14282483

[73] http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?_r=1&mc_cid=6d595ebd14&mc_eid=0%E2%80%A6

[74] https://www.wired.com/2016/05/map-tracks-governments-hack-activists-reporters/?mc_cid=76d56dc5dc&mc_eid=0a14282483